

WHAT IS CLAIMED IS:

1. In an IP network, a method of protecting a host device from a disruptive event, the method comprising the steps of:

receiving a first request from a client for starting a first data connection;

receiving a second request from the client for starting a second data connection;

determining whether the first request and the second request have arrived at the host device within a predetermined time interval, the predetermined time interval being based on a probability distribution function of the arrival times of previous requests for starting data connections received at the host device from a given originating location; and

responsive to the step of determining, denying the second data connection to the client.

2. The method of claim 1, wherein the step of denying further comprises the step of preventing transmission of a synchronize message to the client.

3. The method of claim 1, further comprising the step of storing the first request from the client.

4. The method of claim 3, further comprising the step of storing an originating address of the client.

5. The method of claim 4, further comprising the step of calculating a difference value in the arrival times of the first request and second request at the host device for comparing the difference value to the predetermined time interval.

6. The method of claim 1, further comprising the step of transmitting a signal to a network control center for taking corrective action against the client.

7. The method of claim 6, further comprising the step of barring the client access to the host device by downloading from the network control center appropriate

commands to the server and appropriate commands to specific switching devices in the network.

8. The method of claim 6, further comprising the step of signaling the host device to shut down and the step of sending commands from the network control center to one or more standby servers to take over the processing functions performed by the host device that was shut down.

9. The method of claim 1, further comprising the step of proceeding with establishment of the second data connection if the first request and the second request have arrived at the host device outside of the predetermined time interval.

10. The method of claim 9, wherein the step of proceeding further comprises the step of transmitting a synchronize message to the client.

11. The method of claim 9, further comprising the step of storing an originating address of the client and the arrival time of the second request.

12. The method of claim 1, wherein the disruptive event is a flooding attack.

13. A method of protecting a host device from a flooding event on a telecommunications network, comprising the steps of:

receiving an initializing request from an originating address for initializing a data transmission session;

evaluating whether the originating address for the initializing request has been previously received within a predetermined time value, the predetermined time value being based on a probability distribution function of inter-arrival times of previous initializing requests received at the host device; and

responsive to the step of evaluating, denying the initializing request for the data transmission session.

14. The method of claim 13, wherein the step of denying said request comprises preventing transmission of a synchronizing message to the originating address.

15. The method of claim 13, further comprising the step of saving the originating address and the arrival time of the initializing request.

16. The method of claim 13, wherein the step of denying the request further comprises closing a connection for the data transmission session.

17. The method of claim 13, wherein the step of evaluating further comprises the step of calculating a difference value in arrival times of the initializing request and the previously received initializing request from the originating address.

18. The method of claim 13, further comprising the step of transmitting a signal to a network control center responsive to the step of denying.

19. The method of claim 13, further comprising the step of monitoring a plurality of data packets arriving at the host device so as to generate a probability distribution of the arrival times of a plurality of initializing requests from the originating address.

20. A method of protecting a host device from a flooding event in a telecommunications network, comprising the steps of:

receiving a first request from a client for starting a first data connection;

receiving a second request from the client for starting a second data connection;

determining if a difference value in arrival times of the first request and the second request is less than or equal to a predetermined time period, the predetermined time period being based on a probability distribution function of inter-arrival times of previous requests for data connections received at the host device; and

responsive to the step of determining, denying the second data connection to the client.

21. The method of claim 20, wherein the step of denying further comprises the step of preventing transmission of a synchronize message to the client.

22. The method of claim 20, further comprising the step of allowing the second data connection to proceed if the difference between the arrival times of the first and second requests is greater than the predetermined time period.

23. In a telecommunications network, a system for protecting a host device from a flooding event, the system comprising:

a processing device for processing and receiving a first request from a client for starting a first data session and a second request from the client for starting a second data session; and

a program embodied in computer-readable code cooperating with the processing device to execute steps of receiving the first request from a client for starting the first data connection and the second request from the client for starting the second data connection; evaluating the arrival times of the first request and the second request against a predetermined value based on a probability distribution function fitted to a plurality of inter-arrival times of previous data connection requests received at the host device from a given originating client; and in response to the step of evaluating, denying the second data connection to the client, provided that arrival times of the first request and the second request are at least one of less than and equal to the predetermined value

24. A computer-readable medium having a program in computer-readable code for causing a computer to execute steps to protect a host device from a flooding event, comprising the steps of:

receiving a first request from a client for starting a first data connection;

receiving a second request from the client for starting a second data connection;

evaluating the arrival times of the first request and the second request against a predetermined time value based on a probability distribution function fitted to a plurality of inter-arrival times of data connection requests received at the host device from a given originating client; and

responsive to the step of evaluating, denying the second data connection to the client if the difference of the arrival times of the first request and the second request is less than or equal to the predetermined time value.

25. The computer-readable medium of claim 24, wherein the step of denying the request further comprises the step of preventing transmission of a synchronizing message to the client.

26. The computer-readable medium of claim 25, further comprising the step of storing an IP address of the client.

27. The computer-readable medium of claim 26, wherein the step of storing, further comprises the step of storing the arrival time of the first request.

28. The computer-readable medium of claim 27, wherein the step of evaluating further comprises the step of calculating the difference between the arrival times of the first request and the second request from the client.

29. The computer-readable medium of claim 24, further comprising the step of transmitting a signal to a network control center responsive to the step of denying.

30. The computer-readable medium of claim 24, further comprising the step of monitoring a plurality of data packets arriving at the host device so as to generate a probability distribution of the arrival times.

31. In a telecommunications network, a system for protecting a host device from a flooding event, the system comprising:

means for processing and receiving a first request from a client for initiating a first data session and a second request from the client for initiating a second data session, the first request and the second request having different arrival times at the host device; and

means for determining whether the first request and the second request have arrived within a predetermined time interval based on a probability distribution function of a plurality of inter-arrival times of previous requests for data transmission sessions received at the host device.

32. The system of claim 31, further comprising a means for preventing transmission of a synchronize message to the client responsive to the means for determining.

33. The system of claim 31, further comprising a means for storing an originating address of the client.

34. The system of claim 31, further comprising a means for calculating a difference value in the arrival times of the first request and the second request at the host device.

35. The system of claim 31, further comprising a means for comparing the difference value to the predetermined time interval.

36. The system of claim 31, further comprising a means for transmitting a signal to a network control center responsive to the means for determining.

37. The system of claim 31, further comprising a means for proceeding with the second data connection if the first request and the second request have arrived at the host device outside of the predetermined time interval.

38. The system of claim 37, wherein the means for proceeding further comprises a means for transmitting a synchronizing message to the client.

39. The system of claim 31, further comprising a means for storing the arrival time of the second request.

40. In an IP network, a method of protecting a host device from a flooding event, the method comprising the steps:

receiving a first request from a client for starting a first data connection;

receiving a second request from the client for starting a second data connection;

determining whether the first request and the second request have arrived at the host device within a predetermined time interval, the predetermined time interval being based on a probability distribution function of the arrival times of previous connection establishment requests received at the host device; and

responsive to the step of determining, signaling a network control center.

41. The method of claim 40, further comprising the step of barring the client access to the host device.

42. The method of claim 40, further comprising the step of signaling the host device to shut down.

43. The method of claim 40, further comprising the step of proceeding with establishment of the second data connection if the first request and the second request have arrived at the host device outside of the predetermined time interval.

44. A method of protecting a host device from a flooding event, the method comprising the steps:

receiving a first request from a client for starting a first data connection;

receiving a second request from the client for starting a second data connection;

evaluating the arrival times of the first request and the second request against a predetermined time value based on a probability distribution function fitted to a plurality

of inter-arrival times of data connection requests received at the host device from a given originating client; and

responsive to the step of evaluating, signaling a network control center if the arrival times of the first request and the second request are at least one of less than and equal to the predetermined time value.

45. The method of claim 44, further comprising the step of preventing transmission of a synchronizing message to the client from the host device.

46. The method of claim 45, further comprising the step of storing an IP address of the client.

47. The method of claim 46, wherein the step of storing further comprises the step of storing the arrival time of the first request.

48. The method of claim 443, wherein the step of evaluating further comprises the step of calculating the difference between the arrival times of the first request and the second request from the client.

49. The method of claim 44, further comprising the step of barring the client access to the host device after the network control center is signaled.

50. The method of claim 44, further comprising the step of signaling the host device to shut down.

51. The method of claim 44, further comprising the step of signaling a standby server to take over operations of the host device.